EXHIBIT C-15
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 5 ('661 Patent)	**U.S. 4,669,117 to Van Eck ("Van Eck")**
A cryptographic processing device for securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:57-2:3 – "The present invention is based on the insight to disarrange (to encrypt) in a pseudo-random way the sequence in which the image lines are reproduced on the screen. For that purpose a video terminal according to the invention is characterized by encoding means suited to transform the address combination, which is provided by the central processing unit to address the image store, to another, pseudo-random address combination under the condition that this address combination is unequal to the one provided. For a video receiver located within the radiation field of a terminal thus adapted the realization of technical provisions ordering the radiation received in such a way that recognizable information is reproduced on the screen of said receiver, will be strongly hindered."3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 4:56-60 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(b) a source of unpredictable information;	5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed

	into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(c) a processor:	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(ii) configured to use	3:2-7 – "To make such a reconstruction very difficult or even

said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by randomizing the order of said permutation; and	impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	4:3-11 – "At the output 17 of said converter a serial bit pattern is delivered for each addressed character position of the image store 6, which bit pattern is the digital video signal, which, after having been gated in the logical AND-gate 17, which is controlled by the blanking signal (dps), has to be reproduced on the screen on the image line corresponding to the relevant store line address, and in the image column corresponding to the relevant store column address." 4:35-40 – "With video terminals of the conventional type the digital video signals are delivered at the output of the gate 17 in a 'natural' sequence, so that the signals will be reproduced on the screen line by line and dot by dot in accordance with the conventional analog TV technique." Figure 2.

Claim 6 ('661 Patent)	U.S. 4,669,117 to Van Eck
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	1:57-2:3 – "The present invention is based on the insight to disarrange (to encrypt) in a pseudo-random way the sequence in which the image lines are reproduced on the screen. For that purpose a video terminal according to the invention is characterized by encoding means suited to transform the address combination, which is provided by the central processing unit to address the image store, to another, pseudo-random address combination under the condition that this address combination is unequal to the one provided. For a video receiver located within the radiation field of a terminal thus adapted the realization of technical provisions ordering the radiation received in such a way that recognizable information is reproduced on the screen of said receiver, will be strongly hindered." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 4:56-60 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out." *See also* Louis C. Guillou and Michel Ugon, "Smart Card, A Highly Reliable and Portable Security Device," Crypto '86 at 471 (1986) (identifies security issue for smart cards: "Absolute physical security does not exist, no more for smart cards than for any other computing device."); Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) ("Single-chip smart card processors based on these cores are made by almost all the large silicon foundries . . . .Several marketplace forces are at work to open the smart card as a general-purpose computing platform.").
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming

	part of the control unit 4." Figure 2.
(b) a source of unpredictable information;	5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(c) a processor:	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in

	particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and	3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	4:3-11 – "At the output 17 of said converter a serial bit pattern is delivered for each addressed character position of the image store 6, which bit pattern is the digital video signal, which, after having been gated in the logical AND-gate 17, which is controlled by the blanking signal (dps), has to be reproduced on the screen on the image line corresponding to the relevant store line address, and in the image column corresponding to the relevant store column address." 4:35-40 – "With video terminals of the conventional type the digital video signals are delivered at the output of the gate 17 in a 'natural' sequence, so that the signals will be reproduced on the screen line by line and dot by dot in accordance with the conventional analog TV

	technique." Figure 2.

Claim 7 ('661 Patent)	U.S. 4,669,117 to Van Eck
The device of claim 6 including program logic to activate said expending during said processing.	4:56-5:14 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out. This can be achieved with a video terminal of the sort described in view of FIG. 2 by making the sequence in which the image store 6 is read out deviate from the sequence in which the store line addresses are supplied via the leads 9. To that end an encoding device 29, a code key generator 30 and a controllable switching device 31 are utilized. Under the control of the switch signal at the output 12 the line address leads 9 can be connected, via the two-position switching device 31, at choice either to the input 32 of the encoding device 29 or to the store line address input 33 of the image store 6. The output 34 (eight leads) of the encoding device 29 is connected, via a buffer 35, to said input 33 as well as to the eight address leads 24, which are connected to the latch circuit 23. Owing to this buffer it is prevented that during the reading-in process of the image store 6 the line address information then supplied will also be supplied to the input of the latch circuit 23. Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u."

Claim 11 ('661 Patent)	U.S. 4,669,117 to Van Eck
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	1:57-2:3 – "The present invention is based on the insight to disarrange (to encrypt) in a pseudo-random way the sequence in which the image lines are reproduced on the screen. For that purpose a video terminal according to the invention is characterized by encoding means suited to transform the address combination, which is provided by the central processing unit to address the image store, to another, pseudo-random address combination under the condition that this address combination is unequal to the one provided. For a video receiver located within the radiation field of a terminal thus adapted the realization of technical provisions ordering the radiation received in such a way that recognizable information is reproduced on the screen of said receiver,

	will be strongly hindered." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 4:56-60 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the

	exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(d) a noise production system for introducing noise into said measurement of said power consumption.	5:26–42 – "The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen." 4:56-5:3 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out. This can be achieved with a video terminal of the sort described in view of FIG. 2 by making the sequence in which the image store 6 is read out deviate from the sequence in which the store line addresses are supplied via the leads 9. To that end an encoding device 29, a code key generator 30 and a controllable switching device 31 are utilized. Under the control of the switch signal at the output 12 the line address leads 9 can be connected, via the two-position switching device 31, at choice either to the input 32 of the encoding device 29 or to the store line address input 33 of the image store 6. The output 34 (eight leads) of the encoding device 29 is connected, via a buffer 35, to said input 33 as well as to the eight address leads 24, which are connected to the latch circuit 23. Owing to this buffer it is prevented that during the reading-in process of the image store 6 the line address information then supplied will also be supplied to the input of the latch circuit 23. Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u."

Claim 23 ('661 Patent)	**U.S. 4,669,117 to Van Eck**
A method of securely	1:57–2:3 – "The present invention is based on the insight to

performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	disarrange (to encrypt) in a pseudo-random way the sequence in which the image lines are reproduced on the screen. For that purpose a video terminal according to the invention is characterized by encoding means suited to transform the address combination, which is provided by the central processing unit to address the image store, to another, pseudo-random address combination under the condition that this address combination is unequal to the one provided. For a video receiver located within the radiation field of a terminal thus adapted the realization of technical provisions ordering the radiation received in such a way that recognizable information is reproduced on the screen of said receiver, will be strongly hindered." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 4:56-60 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out."
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(b) generating unpredictable information;	5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will

	be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting between:	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis

	of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(c)(1) performing a computation and incorporating the result of said computation in said cryptographic processing, and	4:56-5:20 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out. This can be achieved with a video terminal of the sort described in view of FIG. 2 by making the sequence in which the image store 6 is read out deviate from the sequence in which the store line addresses are supplied via the leads 9. To that end an encoding device 29, a code key generator 30 and a controllable switching device 31 are utilized. Under the control of the switch signal at the output 12 the line address leads 9 can be connected, via the two-position switching device 31, at choice either to the input 32 of the encoding device 29 or to the store line address input 33 of the image store 6. The output 34 (eight leads) of the encoding device 29 is connected, via a buffer 35, to said input 33 as well as to the eight address leads 24, which are connected to the latch circuit 23. Owing to this buffer it is prevented that during the reading-in process of the image store 6 the line address information then supplied will also be supplied to the input of the latch circuit 23. Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u. In this case the algorithm has to satisfy the conditions that: $a_i \neq a_u$; $a_u \leq (y-1)$, in which y represents the number of screen lines which form the image to be reproduced on the screen; and that there has to be an unambiguous relation between a_i and a_u, in other words, to one value of a_u belongs one and no more than one value of a_i."
(c)(2) performing a computation whose output is not incorporated in said cryptographic processing; and	4:56--5:20 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out. This can be achieved with a video terminal of the sort described in view of FIG. 2 by making the sequence in which the image store 6 is read out deviate from the sequence in which the store line addresses are supplied via the leads 9. To that end an encoding device 29, a code key generator 30 and a controllable switching device 31 are utilized. Under the control of the switch signal at the output 12 the line address leads 9 can be connected, via the two-position switching device 31, at choice either to the input 32 of the encoding device 29 or to the store line address input 33 of the image store 6. The output 34 (eight leads) of

	the encoding device 29 is connected, via a buffer 35, to said input 33 as well as to the eight address leads 24, which are connected to the latch circuit 23. Owing to this buffer it is prevented that during the reading-in process of the image store 6 the line address information then supplied will also be supplied to the input of the latch circuit 23. Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u. In this case the algorithm has to satisfy the conditions that: $a_i \neq a_u$; $a_u \leq (y-1)$, in which y represents the number of screen lines which form the image to be reproduced on the screen; and that there has to be an unambiguous relation between a_i and a_u, in other words, to one value of a_u belongs one and no more than one value of a_i."
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:3-11 – "At the output 17 of said converter a serial bit pattern is delivered for each addressed character position of the image store 6, which bit pattern is the digital video signal, which, after having been gated in the logical AND-gate 17, which is controlled by the blanking signal (dps), has to be reproduced on the screen on the image line corresponding to the relevant store line address, and in the image column corresponding to the relevant store column address." 4:35-40 – "With video terminals of the conventional type the digital video signals are delivered at the output of the gate 17 in a 'natural' sequence, so that the signals will be reproduced on the screen line by line and dot by dot in accordance with the conventional analog TV technique." Figure 2.

Claim 24 ('661 Patent)	**U.S. 4,669,117 to Van Eck**
The method of claim 23 where said selecting is performed in software.	4:56-5:20 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out. This can be achieved with a video terminal of the sort described in view of FIG. 2 by making the sequence in which the image store 6 is read out deviate from the sequence in which the store line addresses are supplied via the leads 9. To that end an encoding device 29, a code key generator 30 and a controllable switching device 31 are utilized. Under the control of the switch signal at the output 12 the line address leads 9 can be connected, via the two-position switching device 31, at choice either to the input 32 of the encoding device 29 or to the store line address input 33 of the image store 6. The output 34 (eight leads) of

	the encoding device 29 is connected, via a buffer 35, to said input 33 as well as to the eight address leads 24, which are connected to the latch circuit 23. Owing to this buffer it is prevented that during the reading-in process of the image store 6 the line address information then supplied will also be supplied to the input of the latch circuit 23. Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u. In this case the algorithm has to satisfy the conditions that: $a_i \neq a_u$; $a_u \leq (y-1)$, in which y represents the number of screen lines which form the image to be reproduced on the screen; and that there has to be an unambiguous relation between a_i and a_u, in other words, to one value of a_u belongs one and no more than one value of a_i."

Claim 25 ('661 Patent)	**U.S. 4,669,117 to Van Eck**
The method of claim 23 where said selecting is performed in hardware on an integrated circuit including a microprocessor.	4:56-5:20 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out. This can be achieved with a video terminal of the sort described in view of FIG. 2 by making the sequence in which the image store 6 is read out deviate from the sequence in which the store line addresses are supplied via the leads 9. To that end an encoding device 29, a code key generator 30 and a controllable switching device 31 are utilized. Under the control of the switch signal at the output 12 the line address leads 9 can be connected, via the two-position switching device 31, at choice either to the input 32 of the encoding device 29 or to the store line address input 33 of the image store 6. The output 34 (eight leads) of the encoding device 29 is connected, via a buffer 35, to said input 33 as well as to the eight address leads 24, which are connected to the latch circuit 23. Owing to this buffer it is prevented that during the reading-in process of the image store 6 the line address information then supplied will also be supplied to the input of the latch circuit 23. Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u. In this case the algorithm has to satisfy the conditions that: $a_i \neq a_u$; $a_u \leq (y-1)$, in which y represents the number of screen lines which form the image to be reproduced on the screen; and that there has to be an unambiguous relation between a_i and a_u, in other words, to one value of a_u belongs one and no more than one value of a_i." *See also* Louis C. Guillou and Michel Ugon, "Smart Card, A Highly Reliable and Portable Security Device," Crypto '86 at 471 (1986)

	(identifies security issue for smart cards: "Absolute physical security does not exist, no more for smart cards than for any other computing device."); Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) ("Single-chip smart card processors based on these cores are made by almost all the large silicon foundries . . . .Several marketplace forces are at work to open the smart card as a general-purpose computing platform.").

Claim 26 ('661 Patent)	**U.S. 4,669,117 to Van Eck**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	1:57-2:3 – "The present invention is based on the insight to disarrange (to encrypt) in a pseudo-random way the sequence in which the image lines are reproduced on the screen. For that purpose a video terminal according to the invention is characterized by encoding means suited to transform the address combination, which is provided by the central processing unit to address the image store, to another, pseudo-random address combination under the condition that this address combination is unequal to the one provided. For a video receiver located within the radiation field of a terminal thus adapted the realization of technical provisions ordering the radiation received in such a way that recognizable information is reproduced on the screen of said receiver, will be strongly hindered." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 4:56-60 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out."
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming

	part of the control unit 4." Figure 2.
(b) generating unpredictable information;	5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 5:10-14 – "Now the encoding device 29 has been adapted in such a

	way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
by selecting a code process from a plurality of code processes, where said selected code process is involved in said cryptographic processing,	5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
but where the value of said outputted quantity is independent of which of said code processes was selected; and	6:16-26 – "In other words, when the encoding device 29 is adapted to convert an address Y supplied to it into a store line address X, the algorithm of the additional encoding device 36 has to be such that the inverse of the algorithm of the encoding device 29, so to speak, will be carried out so that, starting from an address X supplied, the (screen) line address Y will be generated. It appears that often the same algorithm can be used for the two encoding devices 29 and 36, in

	other words, these encoding devices can often have the same structure."
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:3-11 – "At the output 17 of said converter a serial bit pattern is delivered for each addressed character position of the image store 6, which bit pattern is the digital video signal, which, after having been gated in the logical AND-gate 17, which is controlled by the blanking signal (dps), has to be reproduced on the screen on the image line corresponding to the relevant store line address, and in the image column corresponding to the relevant store column address." 4:35-40 – "With video terminals of the conventional type the digital video signals are delivered at the output of the gate 17 in a 'natural' sequence, so that the signals will be reproduced on the screen line by line and dot by dot in accordance with the conventional analog TV technique." Figure 2.

Claim 28 ('661 Patent)	**U.S. 4,669,117 to Van Eck**
A method of securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	1:57-2:3 – "The present invention is based on the insight to disarrange (to encrypt) in a pseudo-random way the sequence in which the image lines are reproduced on the screen. For that purpose a video terminal according to the invention is characterized by encoding means suited to transform the address combination, which is provided by the central processing unit to address the image store, to another, pseudo-random address combination under the condition that this address combination is unequal to the one provided. For a video receiver located within the radiation field of a terminal thus adapted the realization of technical provisions ordering the radiation received in such a way that recognizable information is reproduced on the screen of said receiver, will be strongly hindered." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 4:56-60 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out."

(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(b) generating unpredictable information;	5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(c) using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by randomizing the order of said permutation; and	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4."

	Figure 2." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 5:10-14 – "Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_u." 5:21-42 – "To intensify the encryption process the control unit 4 can be adapted to effect that the algorithm determined by the generator 30 will be changed periodically, e.g. after time intervals each corresponding to a chosen number of image frames. The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen."
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:3-11 – "At the output 17 of said converter a serial bit pattern is delivered for each addressed character position of the image store 6, which bit pattern is the digital video signal, which, after having been gated in the logical AND-gate 17, which is controlled by the blanking signal (dps), has to be reproduced on the screen on the image line corresponding to the relevant store line address, and in the image column corresponding to the relevant store column address." 4:35-40 – "With video terminals of the conventional type the digital video signals are delivered at the output of the gate 17 in a 'natural' sequence, so that the signals will be reproduced on the screen line by line and dot by dot in accordance with the conventional analog TV technique." Figure 2.

Claim 29 ('661 Patent)	U.S. 4,669,117 to Van Eck
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	1:57 – "2:3 – "The present invention is based on the insight to disarrange (to encrypt) in a pseudo-random way the sequence in which the image lines are reproduced on the screen. For that purpose a video terminal according to the invention is characterized by encoding means suited to transform the address combination, which is provided by the central processing unit to address the image store, to another, pseudo-random address combination under the condition that this address combination is unequal to the one provided. For a video receiver located within the radiation field of a terminal thus adapted the realization of technical provisions ordering the radiation received in such a way that recognizable information is reproduced on the screen of said receiver, will be strongly hindered." 3:2-7 – "To make such a reconstruction very difficult or even impossible it is, according to the invention, proposed to disarrange the sequence in which the lines containing character characterizing bit patterns are written on the screen, with due observance of certain restrictive conditions." 4:56-60 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	3:31-43 – "A video terminal designed with an image store thus arranged is diagrammatically shown in FIG. 2, in which 1 designates a central processing unit including an associated programme store for controlling and carrying out in their totality the methods for processing the information signals entering the terminal and leaving it. This processing unit 1 is coupled, via two communication channels 2 and 3, to a control unit which is in its generality indicated by 4. More in particular the channels 2 and 3 (for the exchange of data and the

	exchange of status information) are coupled to an interface 5, forming part of the control unit 4." Figure 2.
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	5:26 – "42 – "The system described above can be adapted in such a way that in response to a read command signal via the output 12 the switching device 31 will be switched in such a way that the leads 9 will be connected to the input 32 of the encoding device 29. In consequence of this it is achieved that the image store 6 will be read out in a line sequence which deviates from the line sequence indicated by the control unit 4. Via the output 34 a store line is pseudo-randomly chosen on the basis of the encryption algorithm introduced, causing at the same time an appropriate vertical deflecting voltage via the leads 24 and the converter 25. Since the encoding device 29 works within the aforesaid conditions of the encryption algorithm, all the screen lines, be it in a pseudo-random sequence, will finally get their turn with the build-up of an image to be reproduced on the screen." 4:56-5:3 – "In order to make such illicit copying of the information reproduced on the screen difficult or practically impossible, it is, according to the invention, proposed to change the standard pattern according to which the image store is read out. This can be achieved with a video terminal of the sort described in view of FIG. 2 by making the sequence in which the image store 6 is read out deviate from the sequence in which the store line addresses are supplied via the leads 9. To that end an encoding device 29, a code key generator 30 and a controllable switching device 31 are utilized. Under the control of the switch signal at the output 12 the line address leads 9 can be connected, via the two-position switching device 31, at choice either to the input 32 of the encoding device 29 or to the store line address input 33 of the image store 6. The output 34 (eight leads) of the encoding device 29 is connected, via a buffer 35, to said input 33 as well as to the eight address leads 24, which are connected to the latch circuit 23. Owing to this buffer it is prevented that during the reading-in process of the image store 6 the line address information then supplied will also be supplied to the input of the latch circuit 23. Now the encoding device 29 has been adapted in such a way that, dependent on an encryption algorithm introduced by the generator 30, an address a_i supplied at the input 32 will be changed into another address a_{ii}.""
(d) outputting said cryptographically processed quantity to a recipient thereof.	4:3-11 – "At the output 17 of said converter a serial bit pattern is delivered for each addressed character position of the image store 6, which bit pattern is the digital video signal, which, after having been gated in the logical AND-gate 17, which is controlled by the blanking signal (dps), has to be reproduced on the screen on the image line

	corresponding to the relevant store line address, and in the image column corresponding to the relevant store column address." 4:35-40 – "With video terminals of the conventional type the digital video signals are delivered at the output of the gate 17 in a 'natural' sequence, so that the signals will be reproduced on the screen line by line and dot by dot in accordance with the conventional analog TV technique." Figure 2.